EMV 3-Dセキュア導入ガイド【附属文書14】に関するFAQ

2026年3月版

クレジット取引セキュリティ対策協議会

1．加盟店における導入・運用に関するFAQ

No.	該当頁	質問	回答
1	－	クレジットカードの加盟店契約はあるものの、例えば、過去1年以上、クレジットカード番号等の取扱いがないEC加盟店についても、EMV 3-Dセキュアの導入の対象となるのか。	過去一定期間におけるクレジットカード番号等の取扱いの有無にかかわらず、原則、EC加盟店はEMV 3-Dセキュアを導入することが求められています。
2	－	EMV 3-Dセキュア以外の不正対策を講じたこと等により、不正が減少傾向にあるEC加盟店においても、EMV 3-Dセキュアの導入が求められるのか。	他の不正対策の実施の有無にかかわらず、原則、EC加盟店はEMV 3-Dセキュアを導入することが求められています。
3	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の最終的な判断については、どの事業者が判断すれば良いのか。	割賦販売法上の不正利用防止措置の義務主体者は加盟店であることから、EMV 3-Dセキュアの導入の判断は一義的には加盟店が行うこととなりますが、クレジットカード番号等取扱契約締結事業者であるアクワイアラー・PSPは、加盟店調査の観点から、加盟店契約の締結・継続・解除の判断において加盟店のEMV 3-Dセキュアの導入状況を考慮することになります。
4	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」に記載された取引の理由をそれぞれ教えてほしい。	**「メールオーダー、テレフォンオーダー取引」「ゲーム機・スマートスピーカー等のEMV 3-Dセキュアが利用できない機器でのEC取引」**については、EMV 3-Dセキュアの仕様上、現時点においては認証ができないため記載しております。 **「個人事業主または法人が契約主体のクレジットカードに限定したサイトでのBtoB取引」「事業者が従業者に行う取引又は事業者が販売代理店に対して行う取引であって、イントラネット環境、IPアドレス等によって通信制限を行っている取引」**については、取引の相手が特定(限定)されており、取引のリスクが著しく低いことから、記載しております。 **「取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」**については、以下のとおりの考え方としております。 **・公共料金（電気、ガス、水道、固定電話）**: 新規申込時には自宅などに直接職員等が往訪し開通手続きをすることが法令や業界自主規制等で義務付けられている。支払方法の手続きには事業者が付番する契約番号等が必要となり、悪意の第三者がなりすますことはできない。万一、不正利用と分かれば、ただちにサービスの利用停止が可能なため不正の発生する蓋然性が極めて低く、現に不正取引が発生していない。 **・国や自治体の請求に基づいて納付する税金・料金・手数料**: 例えば税金は日本国憲法に定める国民の義務として国や地方自治体に届け出がされている先（＝本人が特定されている先）に送付された納付書類をもとに支払手続きが行われる。税金以外でも国や地方自治体の公金は確実な収納事務を行う必要があり、納付者が本人であることの特定が必要である。支払手続きには納付書記載の番号等が必要となるため、基本的には他人が手続きすることはできない。また、現に不正取引が発生していない。 以上を踏まえ、「国や自治体からの請求に基づいて納付する税金・料金・手数料」については以下の3つの要件全てを満たすものについてEMV 3-Dセキュアの未導入が認められる。 ①法令又は条例によって定められた請求であること ②納付後に行われる場合も含めて、取引対象に関して何らかの本人確認の手続きが行われていること ③不正利用が発生していないこと **・保険料・共済掛金**: 生命保険、共済は契約締結時、契約内容変更時、保険料・共済金の請求時に、損害保険は契約締結時・変更時、保険金・返戻金受取時等に取引時の確認として本人確認資料の提示を求めているため本人が特定されており、万一、不正利用と分かればただちに強制解約が可能なため不正の発生する蓋然性が極めて低く、現に不正取引が発生していない。 **・学校教育費（学校教育法で定める「学校」「専修学校」「各種学校」が対象）**: 国、地方自治体などが文部科学省から認可を受けて設置する公立学校や私立学校の学校教育費は、教育基本法・学校教育法において徴収が認められており、支払手続においては入金管理の観点から学生番号や受験番号などを利用して本人の利用であることが確認される運用がなされており、万一、不正利用と分かれば学校から相応の処分がなされるため不正の発生する蓋然性が極めて低く、また、現に不正取引が発生していない。
5	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（2）システムにより特定の者とのみ取引可能な措置が講じられており、なりすましによる不正が発生する蓋然性が極めて低いもの」の「取引具体例」にある「個人事業主または法人が契約主体のクレジットカードに限定したサイトでのBtoB取引」はBtoB取引であれば該当するか。	当該取引具体例については、取引の対象となる事業者向けに提供される専用サイト上での取引の場合であって、利用されるクレジットカードがシステム的な制御により「法人契約カード」の利用に限定、又は取引の対象となる事業者を確認する運用が行われている場合が該当いたします。単にBtoB取引のサイトというだけでは該当いたしません。
6	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（2）システムにより特定の者とのみ取引可能な措置が講じられており、なりすましによる不正が発生する蓋然性が極めて低いもの」について、ID/PWによるアクセス制限を行っている場合は該当するか。	システム的な方法により特定の者とのみ取引可能な措置が講じられているという要件は、一般的なID/PWによるログイン制限のみで満たされるとは想定しておりません。 要件を満たすケースとして2つの具体例をお示ししています。 ・「個人事業主または法人が契約主体のクレジットカードに限定したサイトでのBtoB取引（事業者購買専用サイト、法人間取引専用サイト、宿泊代金精算用の法人契約カード取引等）」は、取引の対象となる事業者向けに提供される専用サイト上での取引の場合であって、利用されるクレジットカードがシステム的な制御により「法人契約カード」の利用に限定、又は取引の対象となる事業者を確認する運用が行われていることが要件となります。 ・「イントラネット環境、IPアドレス等による外部からの通信制限によって利用者を特定することにより、不特定多数の者が利用できない取引（従業員専用サイトでの取引、販売代理店専用サイトでの取引等）」は、イントラネット環境、IPアドレス制限などのシステム的な方法によりサイト自体へのアクセスが特定の者(環境)のみに限定されるクローズドな環境における取引であることが要件となります。
7	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」の「取引具体例」に記載されていないものについても、要件を満たせば対象外として認められるのか。	「取引具体例」に記載されていないものについての「取引対象となる本人が特定されており、不正が発生する蓋然性が極めて低い」取引への該当性については、リスクベースの考え方により、事業者で判断を行うことはあり得ると考えられます。 一方で、「取引具体例」に記載しているものについては、協議会のWGでの検討を重ね、各関係法令や業界の自主ルール等により契約や取引運用時に本人が特定される制約が公に設けられており、実際に不正利用も発生していない取引として「取引対象となる本人が特定されており、不正が発生する蓋然性が極めて低いもの」と判断されたものであり、今後も、必要に応じて見直しを行うことを想定しております。そのことから、各事業者において「取引具体例」に記載しているもの以外のものを導入の対象外と判断するためには、少なくとも上記FAQ №4の回答に記載の考え方と同水準の根拠があることの説明が求められる可能性がある点に留意する必要があります。 また、一定程度の不正利用が発生しているものについては「不正が発生する蓋然性が極めて低い」とは言えないことから、EMV 3-Dセキュアの導入の対象外とはならず、EMV 3-Dセキュアの導入が必要となると考えられます。
8	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」について、本人確認を行わない保険等もあるが、そういったものについてはEMV 3-Dセキュアを導入する必要があるか。	「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」の取引具体例に記載の取引であっても、上記FAQ №4の考え方のとおりの本人確認が行われないものについては、「本人が特定されている」とは言えないことから、EMV 3-Dセキュアの導入の対象外とはならず、EMV 3-Dセキュアの導入が必要となります。 なおオーソリゼーションについてはあくまでカードの有効性の確認となるため、これのみをもって本人が確認されたとは見なされません。
9	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」について、ふるさと納税や寄付は不正利用が発生していることから、EMV 3-Dセキュアを導入する必要があるか。	「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」の取引具体例に記載の取引であっても、ふるさと納税や学校への寄付等、本人が特定されていても不正が発生しているものについては、「不正が発生する蓋然性が極めて低い」とは言えないことから、EMV 3-Dセキュアの導入の対象外とはならず、EMV 3-Dセキュアの導入が必要となります。

No.	該当頁	質問	回答
10	20	「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」の「取引具体例」にある「学校教育費」はどこまでの範囲が未導入と認められるか。	EMV 3-Dセキュアの未導入が認められる「学校教育費」は学校教育法で定める「学校」「専修学校」「各種学校」を対象としていることから、代金の収納先がこれらの教育機関となる取引である事を想定しています。ただし、上記を対象としていても「寄付金」については本人が特定されていても不正が発生しており、「不正が発生する蓋然性が極めて低い」とは言えないことから、EMV 3-Dセキュアの導入の対象外とはならず、EMV 3-Dセキュアの導入が必要となります。
11	20	EMV 3-Dセキュアv2.3では、「ゲーム機・スマートスピーカー等のEMV 3-Dセキュアが利用できない機器でのEC取引」についてもEMV 3-Dセキュアによる認証ができるようになると聞いたが、環境が整った場合は加盟店においてEMV 3-Dセキュアによる認証が求められるのか。	EMV 3-Dセキュアv2.3からは新しい技術環境(IOT、スマートスピーカーなど) への対応がサポートされることから、今後については、市場の状況等を踏まえ、EMV 3-Dセキュア導入ガイドの定期的な見直しの中で検討していく予定です。
12	20	加盟店がカード会社と提携して発行するカード等において、カード入会と同時に加盟店固有のアカウントとカード番号が紐付けされ、会員は当該アカウントにログインするのみで商品・サービスの購入が可能である運用の場合、EMV 3-Dセキュアは対象外でよいか。	割賦販売法の性能規定の考え方においては、「ガイドラインに掲げる措置又はそれと同等以上の措置を講じている場合には『必要かつ適切な措置』が講じられているものと認められる。」ことから、ガイドラインにおける「カードの利用者によるものであるかの適切な確認をイシュアーが行う」という考え方でいうと、イシュアー側でカード入会と同時に加盟店等のアカウント等とカード番号の紐づけを行う場合には、紐づけ時においてEMV 3-Dセキュアによる認証の代替とできる可能性はあり得ます。ただし、各事業者において、EMV 3-Dセキュアと同等以上の措置であることの説明が求められる可能性がある点に留意が必要です。 一方で、決済時には、EMV 3-Dセキュアによる認証を行わなければならないため、当該加盟店サイトにおいてEMV 3-Dセキュアの導入は必要となります。尚、当該サイトがパターン①または②の要件を満たしている場合には、加盟店のリスク判断によりEMV 3-Dセキュア認証を行うことも可能となります。
13	22	「パターン① 加盟店のリスク判断によりEMV 3-Dセキュアによる認証を行う場合」における「PCI DSS準拠で求められる体制整備と同等以上のものとする」について、例示があれば教えてほしい。	PCI DSS準拠で求められる体制整備は多岐にわたりますが、一部の要件について記載しますと以下のような事項が想定されます。 PCI DSSでは安全なシステムの維持、データ保護等で必要となる全ての要件に関するセキュリティポリシーや運用手順の文書化とその最新化、さらに活動を行うための役割と責任の明確化が求められており、それらは最終的に経営層の責任により実行される必要があります。また、インシデントへの即座の対応態勢として、インシデント対応計画の整備、定期的な見直しや訓練、24時間 365日対応可能な担当者の設置が求められます。 これらを不正利用対策に置き換えた場合、企業として対応すべき不正利用対策のポリシーや運用手順が文書化され、常に最新化され、社内の関係者に周知されており、運用において遵守されていること、またそれらの活動が経営層により管理される体制が想定されます。また、急激な不正利用の増加や大規模な不正利用事案の発生時の対応手順が整備されており、定期的な見直しを行うとともに、24時間365日対応可能な担当者の設置が求められることが想定されます。
14	22	「パターン① 加盟店のリスク判断によりEMV 3-Dセキュアによる認証を行う場合」における「本運用はカード会社（アクワイアラー）・PSPの了解の上で行う」について、アクワイアラー・PSPの双方の了解を得る必要があるのか。また、複数のアクワイアラーと契約している場合にはどう考えればよいか。	カード会社（アクワイアラー）・PSPのうち、加盟店契約の最終決定権限を持つ事業者の了解が必要になると考えられます。また、複数のアクワイアラーと契約している場合には、すべてのアクワイアラーの了解が必要となります。
15	23	加盟店等のアカウントへのクレジットカード番号の紐づけの際のEMV 3-Dセキュア認証について、EMV 3-Dセキュアの設定にPA／NPAの項目があるが、NPAで登録時の認証を行う必要があるのか。	NPAはEMV 3-Dセキュアの認証のみ実施し有効性確認のオーソリがされないことから、クレジットカードの有効性が確認されない状態でアカウント登録がされるケースがあるため、本書「EMV 3-Dセキュア導入ガイド」では、カード登録時にもPAを使って認証を行うことを推奨しております。
16	23	「パターン② カード番号登録時にEMV 3-Dセキュア認証を行う場合」について、過去にアカウントに登録されたカードについても遡って認証しなくてはならないのか。	2025年3月以前にアカウントに登録されたカードについて、当該カードが真正利用であることが分かっており、不正利用のリスクがないものについては遡ってEMV 3-Dセキュアによる認証を行う必要はないと考えられます。 ただし、加盟店はアカウント等の利用者であることの確認およびアカウント等の厳格な管理を行う必要はあります。
17	23	「パターン② カード番号登録時にEMV 3-Dセキュア認証を行う場合」に記載の「アカウント等」とは何を指すのか。	アカウント以外にもアプリやデバイス等への紐づけも含まれます。 （例） ・スマホアプリ決済（スマホのアプリやデバイスに紐付けされたクレジットカード情報により実店舗やECの決済を行うもの） ・Wallet決済（Walletのアカウント等に紐付けされたクレジットカード情報によりEC決済を行うもの） ・プリペイドカードのチャージ（口座に紐付けされたクレジットカード情報により利用者の操作でプリペイド残高にチャージするもの） ・手ぶら決済（顔認証等の生体認証技術によりアカウント等に紐付けされたクレジットカード情報により実店舗で決済するもの） なお、スマホアプリへのクレジットカード登録時の加盟店の対策については、附属文書「スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等について」に記載の不正利用対策の実施を推奨しております。
18	23	「パターン② カード番号登録時にEMV 3-Dセキュア認証を行う場合」について、スマートフォン・タブレット等のデバイス上のアプリにクレジットカード番号を登録し、店頭で決済する取引において本運用を行っている。決済の場面でワンタイムパスワードによる認証が難しい場合に、不正リスク判断によってリスクが高いと判断された場合は当該手段での決済は行ってはならないのか。	アプリへのクレジットカード番号の登録時にEMV 3-Dセキュアによる認証を行っていることを前提として、事業者のリスク判断によって決済を行うことは可能です。 なお、スマートフォン・タブレット等のアプリを利用したクレジットカード決済を行う加盟店の不正利用対策については、附属文書「スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等について」に記載の対策の実施を推奨しております。
19	23	「パターン③ 決済の都度、EMV 3-Dセキュアによる認証を行う場合」の運用を行うにあたっては、少額の場合であっても都度のEMV 3-Dセキュアによる認証を行わなければならないのか。	「パターン③ 決済の都度、EMV 3-Dセキュアによる認証を行う場合」の運用を行うにあたっては、取引金額にかかわらず、決済の都度、EMV 3-Dセキュアによる認証を行うことになります。

No.	該当頁	質問	回答
20	23	抽選方式のチケット販売について、抽選申込時と当選時等、一回の取引でEMV 3-Dセキュアによる認証を行うタイミングが複数あるが、どのタイミングでEMV 3-Dセキュアによる認証を行えばよいか。	抽選申込時または当選時のどちらかでEMV 3-Dセキュアによる認証を行っていただくことになります。
21	23	EMV 3-Dセキュアv2.2からサポートされる新仕様により、顧客接点のない取引についてもEMV 3-Dセキュアによる認証ができるようになると聞いたが、そのような新仕様を活用する環境が整った場合は加盟店においてEMV 3-Dセキュアによる認証が求められるのか。	EMV 3-Dセキュアv2.2からサポートされる新仕様（3RI：3dsRequester Initiated）により、EMV 3-Dセキュアの認証が可能となるユースケースもあり、附属文書「【EMV 3-Dセキュア】統合版_AReq設定項目及び3RIの仕様・ユースケース」にユースケースを記載しております。 今後については、市場の状況等を踏まえ、EMV 3-Dセキュア導入ガイドの定期的な見直しの中で検討していく予定です。
22	24	P20の「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」であり、かつ、P24の「加盟店起点の取引における例外」の「クレジットカード番号が通知される取引の次の取引以降に顧客からのクレジットカード番号の通知が行われない取引」の「いわゆる継続課金（リカーリング）取引」である加盟店は、どう考えればよいか。	継続課金（リカーリング）取引は、初回にEMV 3-Dセキュアによる認証を行うことになりますが、P20の「EMV 3-Dセキュアの未導入が認められる取引（導入の対象外）」の「（3）取引対象となる本人が特定されており、なりすましによる不正が発生する蓋然性が極めて低いもの」に記載された公共料金（電気、ガス、水道、固定電話）、国や自治体の請求に基づいて納付する税金・料金・手数料、保険料、共済掛金、学校教育費に関しては、EMV 3-Dセキュアの未導入が認められるため、継続課金（リカーリング）取引であっても初回からEMV 3-Dセキュアによる認証をしないことが可能です。
23	24	「既存取引における加盟店側の事情による再オーソリ」とは具体的に何を指すのか。	以下のような顧客接点のないものを想定しております。 ・商品の一部返品、欠品等による金額変更 ・商品の分割出荷、遅延配送により再オーソリするケース ・宿泊予約でオーソリから販売までが長期間のため再オーソリするケース ・事前予約後の金額確定時決済
24	24	P22の「加盟店起点の取引における例外」の「既存取引における加盟店側の事情による再オーソリ」について、商品の一部返品による金額変更を行う場合に、全額取消・返品のオーソリを行ったうえで、変更後の金額で再オーソリを行う運用をしているが、この場合にEMV 3-Dセキュアによる認証は必要となるか。	取消・返品についてはEMV 3-Dセキュアによる認証をする必要はありません。変更後の金額で再オーソリを行う場合に、その操作を加盟店が行う場合は顧客接点が無いためEMV 3-Dセキュアによる認証は不要となります。
25	24	複数商品の決済が行われる際、顧客視点では同時に決済が行われるが、システム上では商品ごとに個別の決済処理が行われる場合、EMV 3-Dセキュアによる本人認証は1つの商品のみで1度だけ行い、2つ目以降の商品については、加盟店起点の取引となるか。	顧客視点では取引は1件であるため、1つ目の商品の決済処理においてEMV 3-Dセキュアによる本人認証が行われている場合には、2つ目以降の商品の決済処理については加盟店起点の取引として整理され、本人認証を行わないことが認められる余地はございます。 ただし、2つ目以降の商品についてはEMV 3-Dセキュア認証を実施していない取引であるため、オーソリゼーションにCAVV（AAV）を設定できず、原則、加盟店に不正リスクの負担が生じます。なお、実際の運用におけるリスク負担につきましては、ご契約内容により異なってくる場合もございますので、ご契約のカード会社(アクワイアラー)・PSPともご相談ください。
26	47	障害発生時、EMV 3-Dセキュアによる認証を行わずに取引を行うことで、加盟店は割賦販売法35条の17の15等の法令の違反にならないか。	障害が発生していない平時においてEMV 3-Dセキュアを導入されている場合、運用方法によってEMV 3-Dセキュアによる認証を行わない場合においても直ちに法令違反とはなりません。
27	47	障害発生時、EMV 3-Dセキュアによる認証を実施しなかった取引の場合、不正リスク負担はどうなるのか。	リスク負担については、個々の契約関係や、各ブランドルールによって異なります。詳細はご契約のカード会社(アクワイアラー)及びPSPを通じてご確認ください。
28	－	本書について、今後、どのように検討が進められるのか。また、継続的な見直しは行われるのか。	加盟店のEMV 3-Dセキュアの導入・運用の考え方は、割賦販売法に基づく加盟店の不正利用防止義務の履行に関わることから、協議会においてEMV 3-Dセキュアの運用状況及び不正利用被害の発生状況を把握し、経済産業省と協議の上、見直しを行うことを想定しています。

2. その他に関するFAQ

No.	該当頁	質問	回答
1	－	EMV 3-Dセキュア以外の本人認証の手法は認められないのか。	クレジットカード・セキュリティガイドライン6.0版でEC加盟店の指針対策として記載されている「EMV 3-Dセキュアの導入」については、割賦販売法第35条の17の15及び同施行規則第133条の14の規定を踏まえ、加盟店が、クレジットカード番号等の通知を受けた際、当該通知がイシュアーから当該クレジットカード番号等の交付等を受けた利用者によるものであるかの適切な確認をするために必要な措置を講じるものであり、クレジットカード番号等の交付等を受けた利用者によるものであることを確認しうるのはイシュアーのため、その判断はイシュアーが行うこととしており、現時点で考えられるその具体的な手法としてEMV 3-Dセキュアの導入を求めています。 なお、割賦販売法の性能規定の考え方においては、「ガイドラインに掲げる措置又はそれと同等以上の措置を講じている場合には『必要かつ適切な措置』が講じられているものと認められる。」ことから、イシュアーによるカード利用者の確認ができる手法として、EMV 3-Dセキュアと同等以上のセキュリティの措置が講じられている場合であればEMV 3-Dセキュア以外の手法も認められます。（例えばデジタルウォレットの機能を通じクレジットカード番号をトークン化し、当該トークンで決済を行っている場合で、トークン化の際にイシュアーによってプロビジョニングによる本人認証が行われ、さらに決済時にもスマートフォン等での本人認証とオーソリゼーションに設定された認証情報により取引の正当性が検証可能である場合等） ただし各事業者においては、EMV 3-Dセキュアと同等以上の措置であることの説明が求められる可能性がある点に留意する必要があります。
2	－	複数のECサイトを運営している場合、それぞれにEMV 3-Dセキュアの導入が求められるのか。	それぞれのECサイトでEMV 3-Dセキュアの導入をいただきますよう、お願いいたします。
3	－	加盟店が特定の利用者に対し、金額確定後にカード番号とセキュリティコード、有効期限を入れていただくだけのリンクをお送りして決済するような取引（メールリンク型決済）もEMV 3-Dセキュアの導入の対象となるか。	メールリンク型決済もEMV 3-Dセキュアの導入の対象となります。

No.	該当頁	質問	回答
4	-	アプリ内での取引においてもEMV 3-Dセキュアを実装すべきか。	アプリ内決済の非対面取引においても、基本的にEMV 3-Dセキュアの導入が求められます。 実装方法については、加盟店/PSP が、3DS サーバー事業者が提供する 3DS SDK をアプリに実装する方法（App-ベース）と、アプリ内ブラウザを利用してブラウザベースで実装する方法があります。詳しくは、本書「EMV 3-Dセキュア導入ガイド」をご確認ください。また、3DS SDK をアプリに実装する方法（App-ベース）を採用する場合の取引においては、附属文書「スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等について」に記載の不正利用対策の実施を推奨しております。
5	-	デジタルウォレット等にクレジットカード番号を登録し、登録後はクレジットカード番号を利用せず当該デジタルウォレット等で加盟店で決済する取引について、EMV 3-Dセキュアの導入が求められるのか。	デジタルウォレット等による取引についても、原則、EMV 3-Dセキュアの導入が求められますが、デジタルウォレット等による決済を導入する加盟店においては技術的にEMV 3-Dセキュアの導入が出来ないケースが多いと想定されます。このようなケースにおいては実務上はデジタルウォレット事業者が包括的にEMV 3-Dセキュアを導入することになると考えられます。 なお、デジタルウォレットにおけるEMV 3-Dセキュアの導入に関しては、FAQ2-1についてもご参照ください。
6	-	海外発行クレジットカードや法人契約クレジットカード、ハウスカードについてもEMV 3-Dセキュアによる認証が必要なのか。	クレジットカード・セキュリティガイドラインでは、個人向けであるか法人向けであるかを問わず、世界中で共通に使用できるために不正利用リスクが高い、国際ブランド付きのクレジットカードを対象としております。 そのため、国内加盟店で取り扱う海外発行クレジットカードや法人契約クレジットカードでの取引もEMV 3-Dセキュアによる認証の対象となります。 国際ブランドがついていないハウスカードについては対象となりませんが、リスクに応じたクレジットカード番号等の適切な管理及び不正利用の防止のための対策が必要である点に留意が必要です。
7	-	EMV 3-Dセキュアにおける不正利用発生の際のリスク負担はどう考えればよいか。	EMV 3-Dセキュアにおける不正利用発生の際のリスク負担については、国際ブランドルールや加盟店規約等を踏まえ、当事者間で調整いただくことになります。
8	-	加盟店において、国際ブランド付のプリペイドカードやデビットカードについては、どのように対応すればよいか。	プリペイドカード・デビットカードによる取引は割賦販売法が規制する取引の対象外です。一方で、加盟店において当該カード番号がプリペイドカード・デビットカードかクレジットカードかの識別が困難である場合には、加盟店の実務においてはプリペイドカード・デビットカードも併せて対応いただくこととなります。
9	-	イシュアーによって推奨ブラウザ（使用不可ブラウザ）が定義されているのか。	各ACSが推奨環境を規定しており、一般的に利用されるブラウザはサポートされていますが、詳細情報は公開されておりません。
10	-	不正顕在化加盟店になった加盟店に対して、Merchant ID、MCCの変更及び、AReqオプション項目の設定、個人情報属性の同意画面の確認などの周知は、どの事業者が実施するのか。	アクワイアラーが起点となり、直接契約先の加盟店である場合は当該加盟店に、包括契約加盟店である場合は PSPを通じてそれぞれ要請を行うことになります。
11	-	PAとNPAの違い或いは、利用する際の注意点などはあるか。	PAとNPAの違いはEMV 3-Dセキュア導入ガイドの第4章（2）の記載を参照ください。 留意事項として、クレジットカード登録時の認証においては、不正取引も頻繁に発生していることからNPA ではなく、PA を使用する必要があります。また、EMV 3-Dセキュア認証に加えてカード有効性確認のオーソリゼーション等を実施することを推奨いたします。
12	-	「5.EMV 3-Dセキュア導入加盟店における個人情報保護法の遵守に関する留意点」について、イシュアーとして会員規約の変更等の対応をする必要があるのか。	加盟店の「同意取得文言例」による第三者提供の同意取得がなされている場合、情報主体から加盟店への委託等の構成がとれ、イシュアーの確認記録義務は適用されません。その他個人情報保護法の対応(例：利用目的の特定)について、各社の現状の規約等で充足されている場合は不要です。不足している場合には補っていただく必要がありますが、最終的には、各社の法務部門による判断を推奨いたします。
13	-	カードを所持している利用者に対してのEMV 3-Dセキュアの普及率を教えてほしい。	これまで、カード会社（イシュアー）に対して、2025年3月末時点で、各社のEC利用カード会員ベースで80%の会員にEMV 3-Dセキュアの利用登録を推進するように求めてまいりました。同様に2025年3月末時点で動的(ワンタイム)パスワード等による認証の実施がEMV 3-Dセキュア登録会員ベースで100%となるよう対応を求めてまいりました。 2025年4月以降においても、引き続き各カード会社（イシュアー）にて上記の登録率の維持に取り組むよう求めてまいります。